CLAIMS

1. A method of protecting a cryptographic algorithm (6) for execution in a device (1) comprising programmable processor unit (4), the algorithm being separable into the form of initial polynomials (P_i) of at least two variables each, and having a degree of not less than two, the method being characterized in that it comprises the steps of providing combined polynomials (Q_k) each obtained from at least two initial polynomials (P_i, P_{i+1}), and of implementing the combined polynomials (Q_k) in the programmable processor unit (4).

2. A method according to claim 1, characterized in that it further comprises the step of storing the combined polynomials (Q_k) in the form of a configuration file that is loaded into a memory (3) associated with the processor unit (4).

3. A method according to claim 2, characterized in that the memory (3) and the programmable processor unit (4) are associated with an eraser member (5) serving, in the event of an intrusion into the device, to erase the processor unit (4), and to erase the memory (3) containing the configuration file when the configuration is present in said memory.

4. A method according to claim 1, characterized in that it includes the step of combining each combined polynomial (Q_k) with a function (f_k), and of combining the following combined polynomial (Q_{k+1}) with an inverse function (f_k^{-1}).

5. A method according to claim 4, characterized in that the function (f_k) combined with each combined polynomial (Q_k) is a linear function.